代数仕様言語 CafeOBJ による 鉄道信号システムの記述

清野 貴博

北陸先端科学技術大学院大学 情報科学研究科

1999 年 2 月 15 日

キーワード: 形式手法, 形式仕様, 検証, CafeOBJ, 鉄道信号.

1 研究の目的

鉄道信号は大規模な分散型のシステムのうち、最も成功している事例の一つである。鉄道信号において、重要な概念は「閉そく (Block system) 」と「連動 (Interlocking) 」である。閉そくとは、線路をいくつかの区間に区切り、その区間を一列車に占有させるという考え方である。連動とは、個々の装置の間の関係を決めるもので、ある装置を取り扱った時に、別の装置を取り扱うことができないようにする「鎖錠関係」を持たせ、それを保ちながら動作することを言う。

鉄道信号のドメインでは、閉そくを実現するための方法や、鎖錠関係の分類などは、古くから整理されている。これらの概念を、分散オブジェクトモデルが扱える代数仕様言語である CafeOBJ を用いて記述・検証し、鉄道信号における形式仕様の有効性について示すことを第一の目的とする。

現在、鉄道信号における形式仕様の適用の多くは、駅構内の連動論理設計に集中している。駅構内には多数の進路を持つ線路や、それに付随する信号機が林立し、その設計は困難であることが知られており、そのため形式手法による支援が研究されている。それらの多くは、対象となる駅とその線路配置を特定し、それについて仕様を記述し、シミュレーションによって安全性を検証する。我々はこれに対し、信号システムのスキームそのものを記述し、線路配置を特定せずに、スキームの段階で安全性を検証する。これによって、安全な信号システムのスキームから具現化される、あらゆる鉄道システムも安全に機能する、という新しい設計手法の確立を目指す。

2　研究に用いた手法

本研究では、仕様記述言語として、代数仕様言語 CafeOBJ を選択した。CafeOBJ は代表的な代数仕様言語である OBJ を祖とし、強力なモジュールシステム、順序ソート代数 (Order Sorted Algebra) 、隠蔽代数 (Hidden Algebra) によるオブジェクトモデルのサポート、項書換えによる仕様の実行など、様々な機能を備えた先進的な言語である。

隠蔽代数によるオブジェクトは、オブジェクトの状態を変化させる操作演算 (Action) とオブジェクトの状態を得ることができる観測演算 (Observation) によって表現される。操作演算と観測演算の間の関係は、任意の回数、任意の観測演算を適用した後に、操作演算を一回だけ行うという観測文脈によって定義する。このようにして書かれた仕様を振舞仕様 (Behavioural Specification) と呼ぶ。

振舞仕様において、オブジェクトの等価関係は観測によってのみ定義される。二つのオブジェクトが持つそれぞれの観測演算の結果が等しく、それに操作演算を適用した後の観測も等しいならば、二つのオブジェクトは振舞等価 (Behavioural Equivalence) であると言う。

オブジェクトを組み合わせて大きなオブジェクトを作る合成は、射影演算 (Projection) によって定義する。射影演算は合成後のオブジェクトの状態を、合成前の個々のオブジェクトの状態空間にマップする演算である。振舞等価なオブジェクト同士を射影演算によって合成したオブジェクトは元のオブジェクトの振舞等価性を再利用して、合成後のオブジェクトの振舞等価であることを証明することができる。

振舞仕様の振舞等価性を操作演算の文脈による帰納法によって証明するのは、大きな仕様では困難であるので、隠蔽合同関係を定義することによって振舞等価性を証明する余帰納法を利用して、様々な性質を示すことにする。

3　研究の成果

本研究では、我が国の鉄道で使用されている鉄道信号システムを対象とし、そこで用いられている閉そくの概念とその実現法について記述した。

複線区間の信号システムは、レール、列車、軌道回路 (Track Circuit) 、信号機の各オブジェクトを合成して記述した。複線区間においては、上り線、下り線のように列車進行方向が固定のため、列車同士の追突を防止することを考える。まず、レールを連続した閉そく区間に分割し、各区間にはその区間に列車がいるかどうかを検出する軌道回路を設置する。各区間の始端には信号機を設置し、その区間に列車がいれば停止信号を、いなければ進行信号を現示し、後続の列車に区間の状況を知らせる。また、今日では停止信号と進行信号だけではなく、高速、高密度運転に対応するため、停止信号を予告する注意信号なども使用されているため、それらの信号を含めた閉そくシステムを記述し、線路の長さや閉そく区間の数などに依存せず、閉そくが保たれていることを余帰納法により証明した。

単線区間の信号システムでは、一本の線路上を双方向に列車が走るため、無秩序に列車

が走ると正面衝突の危険がある。そこで、複線区間の設備の他に、列車交換のための設備と、どちらの方向に列車を運転するのかを決める方向てこが必要になる。そこで、これらのオブジェクトを複線区間の信号システムに加え、正面衝突が起こらないこと、閉そくが保たれていることを、同様に余帰納法により証明した。

これらの仕様は限定的ではあるが、具体的な線路配置に依存しないように記述した。本研究では、これら証明済みの信号付き線路コンポーネントを組み合わせて、鉄道システムを作り上げるための足がかりを示した。